Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

The Impact of Information Security Rating on Vendor Competition

Zach Z. Zhou
Dartmouth College, zach.zhou@tuck.dartmouth.edu

Eric M. Johnson
Dartmouth College, m.eric.johnson@tuck.dartmouth.edu

The Impact of Information Security Rating on Vendor Competition

Zach Z. Zhou
Center for Digital Strategies
The Tuck School of Business
Dartmouth College
zach.zhou@tuck.dartmouth.edu

M. Eric Johnson
Center for Digital Strategies
The Tuck School of Business
Dartmouth College
m.eric.johnson@tuck.dartmouth.edu

ABSTRACT

Security breaches often stem from business partner failures within the value chain. There have been several recent efforts to develop a common reference for rating the information risk posed by partners. We develop a simple analytical model to examine the impact of such information security ratings on service providers, customers, and social welfare. While some might believe that ratings would benefit high-security providers and hurt those with lower security, we show that this is not always the case. We find that information security ratings can hurt both types of providers or benefit both, depending on the market conditions. Surprisingly, we also find that security ratings do not always benefit the most demanding customers who desire highly secure business partners. Yet, in all cases, we find that social welfare is improved when information security ratings are adopted. This result suggests that information security ratings should be encouraged through public policy initiatives.

Keywords

Economics of Information Security, Information Security Rating, IT Policy and Management, Information Systems.

1. INTRODUCTION

Outsourcing has been widely adopted in many industries. Within the IT function, the benefits of subcontracting business processes have been widely discussed including cost reduction, improved utilization of core IS resources, and the acquisition of new technical skills and competencies (DiRomualdo and Gurbaxani 1998). Recent technology innovations allowing increased network bandwidth, processing virtualization, and inexpensive storage have pushed outsourcing to a new level by facilitating the migration of many internal IT applications to externally provided services. In this so called Software as a Service (SaaS) model, business applications are provided on demand as a service to customers. SaaS allows firms to reduce many fixed costs associated with the required internal IT infrastructure, application deployment, testing, maintenance, and patch management. It also lowers cost through competition. If a firm is not satisfied with a service provider, they can switch to another provider without losing significant upfront investments (those investments would represent a sunk cost if the firm had entered into a long-term contract with an outsourcing vendor). Furthermore, enterprises using a service-oriented architecture (SOA), can segment different processes and outsource them to different service providers. For example, within the financial services industry, many institutions rely heavily on both traditional outsourcing and SaaS, employing thousands of vendors that support their business processes.

While these different forms of outsourcing provide enterprise customers with both flexibility and cost benefits, the use of external service providers handling sensitive business data introduces new security risks. Many widely publicized security breaches have been the result of a partner failure (Macura and Johnson 2009). Sometimes these failures stem from neglect or under-investment in security. In other cases, the security challenges arise from the nature of service provider's business model. Providers who frequently enhance their service offering in response to evolving customer demand, introduce the possibility of new security bugs with every additional feature. Traditional methods in software assurance, with significant code testing, can be time consuming, slowing the vendor's ability to compete and tempting them to cut corners.

Of course a second worry is the firm's sensitive data that may be stored on a service provider's machines and handled by employees of the service provider. That data represents a significant risk because the firm no longer has the ability to directly monitor and control its access. Even if the vendor's network is secure, the firm faces many web-based threats (hacking, malicious code etc.) when data is moving from the service provider's facility over the Internet. Lastly, service providers often employ a model of multi-tenancy, where many enterprise customers share the same business application infrastructure with

controlled access to their own data. The challenge for the service provider is segregating the data of customers. Inadequate data management may allow one firm's data to be exposed to another customer, which may be a competitor in the same industry.

For all of these reasons, firms must assess the information security level of their partners. Traditionally, customers perform such assessments through surveys, interviews, on-site visits, testing, and document review. Using that information the customers typically develop their own risk assessment (through identification of threats and vulnerabilities, control analysis, likelihood determination, risk determination etc.) (Stoneburner et al. 2002). This is time-consuming and costly activity for both vendors and customers. Since many firms (especially those in the financial industry) have hundreds of service providers, the time required to perform the risk assessment can make it impossible to assess every critical service provider.

Recently there have been several efforts to develop a common risk rating including the BITS shared assessment, security vendor assessments (like Symantec's IT Risk Assessment) and most recently the collaboration between Goldman Sachs, Moody's, and Avior to create a Vendor Information Risk Rating (VIR). For example, in the Moody's rating, service providers who sign up are analyzed and rated in 11 "security fundamentals" categories, including access control, business continuity and data security. Two types of ratings are assigned to service providers - overall security quality ratings and inherent risk ratings. The idea behind such ratings is to reduce the burden for both enterprise customers and service providers by creating a single efficient risk rating (Kark 2008) that can be used by many (rather and each firm individually assessing each of their vendors)

Kliger and Sarig (2000) examined security price reactions to Moody's refinement of its rating system and found that rating information was valuable. While prior financial literature assumes that credit rating benefits the high-credit issuer while hurts the low-credit issuer (Kliger and Sarig 2000), we want to examine whether this classical insight can be readily applied to the risk rating in the IS field, where the vendor competition can be affected by the risk rating.

In this paper, we develop an analytical model to examine the impact of information security rating on service providers, customers, and social welfare. We do this by comparing two cases: (1) the case where an information security rating is provided, and (2) the case where it is not provided. While it is tempting to directly equate information security rating with ratings of financial instruments, security ratings are quite different from credit ratings (which measure the default probability for a debt issuer). A good credit rating generally enables the debt issuer to raise money from the financial market at a lower cost. However, a good security rating does not necessarily benefit a high-security service provider because the security rating may have subtle impacts on the competition among service providers, their incentives to improve security levels, and their prices charged to customers. For example, it is commonly believed that information security ratings benefit high-security service providers (and conversely hurts low-security providers). However, we find a surprising result: information security ratings can hurt or benefit both types of service providers, depending on the market conditions. Likewise, our analysis leads to another counterintuitive result: information security rating can hurt demanding customers. Prior results in the licensing literature claimed that improved information always benefits the high-needs customers at the cost of less demanding customers (Shapiro 1986). We find cases where that is not true for information security.

We begin by examining the related literature. In Section 2, we present our model. We analyze the case with and without ratings in Sections 4-5. We then conclude with recommendations for researchers and policy makers.

LITERATURE REVIEW

A growing literature has examined the economics of information security from several different perspectives. Gal-Or and Ghose (2005) examined the value of information sharing about security breaches between competing firms. Kannan and R. Telang (2005) compared a market-based mechanism and a Computer Emergency Response Team (CERT) mechanism for vulnerability disclosure. They found that the former mechanism almost always underperforms the latter one. Arora, Telang and Xu (2008) further examined CERT's optimal timing of disclosing a vendor's software vulnerability. They found that the vendor may release the patch later than is socially optimal when there is no forced disclosure. Thus, social planners could push the vendor to release the patch more quickly by threatening to disclose its software vulnerabilities. Arora, Caulkins, and Telang (2006) used an analytical model to show that a software vendor may have incentives to release buggier software early and patch it later in a larger market. August and Tunca (2006) examined alternative policies to manage network security in a network where vulnerabilities exhibit negative network externalities. They showed how the most effective policy is determined by the security risk and patching costs. August and Tunca (2008) further studied whether the users of unlicensed software should be provided the ability to apply security patches. They showed how the joint effects of software piracy and negative network security externalities affect the optimal policy choices. We examine the effects of vendor information security rating, which was not directly addressed in these papers.

2. THE MODEL

We adopt a vertical differentiation framework (see, for example, Bhargava and Choudhary [2001, 2008]) for customers who have different usage utilities for a business application service. We model two risk-neutral representative customers: (1) low-type customer, whose usage utility from using the business application service is $V > 0$, and (2) high-type customer, whose usage utility from using the business application service is θV with $\theta > 1$.

A service provider exerts effort e ($e \in [0,1]$) to increase the information security level of its service offering. We normalize the threat probability, the probability that the vendor is breached, to $1-e$. That is, when the service provider exerts greater efforts, it is less likely to be breached. The fixed cost of exerting effort e on security is assumed to be a convex function: ce^2, where $c > 0$ is the security cost parameter (Bhargava and Choudhary 2001). Consistent with prior literature (August and Tunca 2006), when a breach occurs, the customer incurs a loss proportional to its usage utility. We use λV and $\lambda\theta V$ to denote the loss of the low-type customer and the high-type customer respectively, where $0 < \lambda < 1$.

ASSUMPTION 1: To focus on the interior solution, we assume that $V\theta\lambda / c < 1$, which ensures that the optimal efforts of both the low-security service provider (e_l^*) and high-security service provider (e_h^*) are less than 1.

Two service providers engage in a two-period competition. The sequence of events are as follows. In Period 0, the service providers determine their efforts on security level. If an information security rating is provided in Period 1, the customers will know the efforts (or security levels) of both service providers. However, if a rating is not provided in Period 1, then the security levels of both service providers are unobservable to customers in Period 1. However, in time customers will eventually know the service providers' security levels in Period 2 via the customers' individual assessments or a reputation mechanism (e.g. academic publications, newspaper, word-of-mouth among customers etc.). This means that the information security rating agencies are more efficient than individual customers or the reputation mechanism (Kark 2008).

Both service providers announce their prices in both periods; customers make choices based on their preferences and the information available to them.

For ease of exposition, we use e_l and e_h to denote lower and higher effort (or security level) respectively. p_l and p_h denote lower and higher price charged by service providers. π_l and π_h denote the total profit of lower and higher-security service provider in both periods. Next we analyze two cases: (1) an information security rating is provided in Period 1, and (2) a rating is not provided in Period 1.

3. Competition with Information Security Rating

Information security ratings reveal the efforts of service providers to customers in Period 1. Hence, customers know e_l and e_h in both periods. The competition in Period 1 is the same as that in Period 2. Hence, in Period 2, a service provider charges the same price as that charged in Period 1; a customer chooses the same service provider as that chosen in Period 1. Thus, we only need to focus on a single period.

We use $U(t,s,p)$ to denote the net surplus of a type-t customer who uses a business application service with a security level of s and a price of p, where $t = t_L$ (low-type customer) or t_H (high-type customer); $s = s_L$ (lower security level) or s_H (higher security level); $p = p_l$ or p_h. The expressions of $U(t,s)$ are as follows.

$$U(t_L, s_L, p_l) = e_l(V - p_l) + (1-e_l)\left[(1-\lambda)V - p_l\right]$$
$$U(t_L, s_H, p_h) = e_h(V - p_h) + (1-e_h)\left[(1-\lambda)V - p_h\right]$$
$$U(t_H, s_L, p_l) = e_l(\theta V - p_l) + (1-e_l)\left[(1-\lambda)\theta V - p_l\right]$$
$$U(t_H, s_H, p_h) = e_h(\theta V - p_h) + (1-e_h)\left[(1-\lambda)\theta V - p_h\right]$$

If both service providers stay in the market (i.e. high-security service provider sells to the high-type customer while low-security service provider sells to the low-type customer), then the low-security service provider can capture the low-type customer by charging a price p_l such that (IC1) $U(t_L, s_L, p_l) \geq U(t_L, s_H, p_h)$ (the low-type customer chooses the low-security

service provider rather than the high-security service provider) and (IR1) $U(t_L, s_L, p_l) \geq 0$ (the low-type customer does not suffer a loss from using the service of the low-security service provider). Similarly, the high-security service provider should charge a price p_h such that (IC2) $U(t_H, s_H, p_h) \geq U(t_H, s_L, p_l)$ and (IR2) $U(t_H, s_H, p_h) \geq 0$.

It can be shown that both IR1 and IC2 are active and that IR2 and IC1 can be neglected. Using IR1 and IC2, we get

$$\begin{aligned} p_l &= V(1-\lambda+\lambda e_l) \\ p_h &= V\theta\lambda(e_h - e_l) + V(1-\lambda+\lambda e_l) \end{aligned} \tag{1}$$

The total profits of high-security service provider and low-security service provider in two periods can be written as follows.

$$\begin{aligned} \pi_l &= 2p_l - ce_l^2 \\ \pi_h &= 2p_h - ce_h^2 \end{aligned} \tag{2}$$

Inserting (1) in (2) and solving the first-order condition (F.O.C.) for optimal efforts, we obtain e_l^* and e_h^*. The second order conditions are satisfied because $d^2\pi_l / de_l^2 = d^2\pi_h / de_h^2 = -2c < 0$.

Proposition 1. When an information security rating is provided to customers in the first period, then the optimal efforts of high-security and low-security service provider to enhance security level are given by

$$\begin{aligned} e_l^* &= V\lambda / c, \\ e_h^* &= V\theta\lambda / c. \end{aligned}$$

The prices and profits of both service providers are given by $p_l^* = V\left[1-\lambda(1-V\lambda/c)\right]$, $p_h^* = V^2\lambda^2\theta(\theta-1)/c + V\left[1-\lambda(1-V\lambda/c)\right]$, $\pi_l^* = V\left[2-\lambda(2-V\lambda/c)\right]$, $\pi_h^* = V^2(\theta-1)^2\lambda^2/c + V\left[2-\lambda(2-V\lambda/c)\right]$.

Next, we show that the high-security service provider does not have any incentives to compete the low-security service provider out of the market in equilibrium. If that happened, both types of customers would choose the high-security service provider even though the low-security service provider charges $p_l = 0$. That is, the high-security service provider must charge a price such that $U(t_L, s_H, p_h) \geq U(t_L, s_L, p_l)|_{p_l=0}$, $U(t_H, s_H, p_h) \geq U(t_H, s_L, p_l)|_{p_l=0}$. This leads to $p_h \leq \min\left[V\theta\lambda(e_h^* - e_l^*), V\lambda(e_h^* - e_l^*)\right] = V\lambda(e_h^* - e_l^*)$. Hence, if the high-security service provider charges $p_h = V\lambda(e_h^* - e_l^*)$, it will obtain a profit of $\pi_h = 4p_h - c(e_h^*)^2$ instead of $\pi_h^* = 2p_h^* - c(e_h^*)^2$. However, $\pi_h^* - \pi_h = \frac{2V}{c}\left[c(1-\lambda) + V\lambda^2(\theta^2 - 3\theta + 3)\right] > 0$ given $0 < \lambda < 1$ and $\theta > 1$. Therefore, two service providers share the market in equilibrium as shown in Proposition 1.

4. Competition without Information Security Rating

In this section, we examine the case of competition where no information security rating is provided. We focus on the rational expectations equilibrium (Muth 1961), where customers form expectations on security levels of service providers, and the expectations are unbiased in equilibrium. That is, $E(e_l^*) = e_l^*$ and $E(e_h^*) = e_h^*$. The efforts of service providers remain unknown to customers in Period 1. Thus, both service providers appear identical to customers, and they charge the same introductory price p_i; customers randomly choose a service provider in Period 1. We use $U(t, p)$ to denote the net surplus of a type-t customer who randomly chooses a service provider.

$$\begin{aligned} U(t_L, p_i) &= \frac{1}{2}E\left[U(t_L, s_L, p_i)\right] + \frac{1}{2}E\left[U(t_L, s_H, p_i)\right], \\ U(t_H, p_i) &= \frac{1}{2}E\left[U(t_H, s_L, p_i)\right] + \frac{1}{2}E\left[U(t_H, s_H, p_i)\right], \end{aligned}$$

where $E\left[U\left(t_L, s_L, p_i\right)\right] = E\left(e_l\right)\left(V - p_i\right) + \left(1 - E\left(e_l\right)\right)\left[\left(1-\lambda\right)V - p_i\right]$, $E\left[U\left(t_L, s_H, p_i\right)\right] = E\left(e_h\right)\left(V - p_i\right) + \left(1 - E\left(e_h\right)\right)\left[\left(1-\lambda\right)V - p_i\right]$, $E\left[U\left(t_H, s_L, p_i\right)\right] = E\left(e_l\right)\left(\theta V - p_i\right) + \left(1 - E\left(e_l\right)\right) \times \left[\left(1-\lambda\right)\theta V - p_i\right]$, $E\left[U\left(t_H, s_H, p_i\right)\right] = E\left(e_h\right)\left(\theta V - p_i\right) + \left(1 - E\left(e_h\right)\right)\left[\left(1-\lambda\right)\theta V - p_i\right]$.
There are two possible scenarios in equilibrium: (S1) only the high-type customer can afford the introductory price p_i in Period 1, and (S2) both types of customers can afford p_i in Period 1.

In the first scenario (S1), the expected demand of each service provider is $\frac{1}{2}$. The introductory price p_i is set to satisfy $U\left(t_H, p_i\right) = 0$, or $p_i = V\theta\left(1-\lambda\right) + \frac{1}{2}\lambda\theta V\left[E\left(e_l\right) + E\left(e_h\right)\right]$. In Period 2, service providers charge different prices (p_h and p_l) because their efforts on security are revealed to customers via a reputation mechanism. Using a similar argument as that in Section 3, we get $p_l = V\left(1-\lambda+\lambda e_l\right)$ and $p_h = V\theta\lambda\left(e_h - e_l\right) + V\left(1-\lambda+\lambda e_l\right)$. The profits of low-security and high-security service providers can be expressed as: $\pi_l = \frac{1}{2}p_i + p_l - ce_l^2$ and $\pi_h = \frac{1}{2}p_i + p_h - ce_h^2$. We obtain the optimal efforts by solving the first order conditions of service providers.

In the second scenario (S2), the expected demand of each service provider is 1. The introductory price p_i satisfies $U\left(t_L, p_i\right) = 0$, or $p_i = V\left(1-\lambda\right) + \frac{1}{2}\lambda V\left[E\left(e_l\right) + E\left(e_h\right)\right]$. In Period 2, service providers charge p_l and p_h respectively when their efforts are revealed. The profits can be expressed as: $\pi_l = p_i + p_l - ce_l^2$ and $\pi_h = p_i + p_h - ce_h^2$. Again, we obtain the optimal efforts by solving the F.O.C. It can be shown that the second order conditions are satisfied.

Comparing the maximum profits obtained from S2 and from S1, we find that when $\theta > 2$, the maximum profits of both service providers in S1 are greater than those in S2. We summarize the results in the following proposition. The detailed proof is in the Appendix.

Proposition 2. When $\theta > 2$, the optimal efforts of high-security and low-security service provider to enhance security level are given by

$$e_l^* = V\lambda\left(4+\theta\right)/\left(8c\right),$$
$$e_h^* = 5V\theta\lambda/\left(8c\right).$$

The prices and profits of both service providers are given by $p_i^* = \frac{V\theta}{8c}\left[8c\left(1-\lambda\right) + V\lambda^2\left(2+3\theta\right)\right]$, $p_l^* = \frac{V}{8c}\left[8c\left(1-\lambda\right) + V\lambda^2\left(4+\theta\right)\right]$, $p_h^* = \frac{V}{8c}\left[8c\left(1-\lambda\right) + V\lambda^2\left(4+4\theta^2-3\theta\right)\right]$, $\pi_l^* = \frac{V}{64c} \times [32c\left(2+\theta\right)\left(1-\lambda\right) + V\lambda^2\left(11\theta^2+8\theta+16\right)]$, $\pi_h^* = \frac{V}{64c}\left[32c\left(2+\theta\right)\left(1-\lambda\right) + V\lambda^2\left(19\theta^2-16\theta+32\right)\right]$. Only the high-type customer can afford p_i^* in Period 1.

When $1 < \theta \le 2$, the optimal efforts of high-security and low-security service provider to enhance security level are given by

$$e_l^* = 3V\lambda/\left(4c\right),$$
$$e_h^* = V\lambda\left(1+2\theta\right)/\left(4c\right).$$

Both service providers only sell to the high-type customer in Period 1. The prices and profits of both service providers are given by $p_i^* = \frac{V}{4c}\left[4c\left(1-\lambda\right) + V\lambda^2\left(2+\theta\right)\right]$, $p_l^* = \frac{V}{4c}\left[4c\left(1-\lambda\right) + 3V\lambda^2\right]$, $p_h^* = \frac{V}{4c}[4c\left(1-\lambda\right) + V\lambda^2\left(2\theta^2-2\theta+3\right)]$, $\pi_l^* = V\left[2\left(1-\lambda\right) + V\lambda^2\left(11+4\theta\right)/\left(16c\right)\right]$, $\pi_h^* = V\left[2\left(1-\lambda\right) + V\lambda^2\left(4\theta^2-8\theta+19\right)/\left(16c\right)\right]$. Both types of customers can afford p_i^* in Period 1.

When information security ratings are not available, service providers appear identical to customers. Thus, the service providers cannot segment the market by selling to different types of customers. Instead, service providers have the same chance to sell to a specific type of customer. When the high-type customer has sufficiently high willingness-to-pay for the business application service (θ sufficiently large, $\theta > 2$), the target customer is high-type customer only. Otherwise, target customers are both types of customers.

5. Comparison: with Information Security Rating and without Information Security Rating

We use Case NR to denote the case where the information security rating is not provided in Period 1, and Case R to denote the case where the information security rating is provided in Period 1.

Free-riding arises in Case NR because the low-security service provider can claim to be a "high-security service provider".

Intuitively, the free-riding problem should reduce the high-security service provider's incentive to invest in security. But, it is not obvious how the low-security service provider's security effort is affected. There are two conflicting effects. First, the low-security service provider appears identical to the high-security service provider in Period 1, so it could have incentives to enhance its security level to increase the willingness-to-pay of customers. Second, the low-security provider still needs to maintain an appropriate differentiation with the high-security provider in Period 2 to avoid an intense price competition after efforts are known to customers. Since the free-riding reduces the high-security provider's effort on security, the low-security provider could also reduce its effort to keep an appropriate differentiation with the high-security provider.

Proposition 3. When an information security rating is not available, free-riding reduces the security effort of the high-security service provider. It also reduces the security effort of the low-security service provider when $1 < \theta \le 4$, but increases its effort when $\theta > 4$.

When $\theta > 2$, only the high-type customer can afford the introductory price (p_i^*) in Period 1 of Case NR (see Proposition 2). In Period 1 of Case NR, the low-security service provider sells to the high-type customer instead of the low-type customer (in Case R). When the high-type customer's taste is sufficiently large ($\theta > 4$), the low-security service provider will increase its effort on security because the gains from the high-type customer in Period 1 exceeds the loss from a narrower differentiation between the two service providers, which can cause intense price competition in Period 2.

Proposition 4. The information security rating benefits both service providers when $\theta < \frac{5}{4}$. It hurts both service providers when $\theta > 2$ and $c > \frac{V\lambda^2\left[96+(45\theta-112)\theta\right]}{32(\theta-2)(1-\lambda)}$. It benefits the high-security service provider but hurts the low-security service provider in other regions.

It might seem intuitive that the information security rating always helps the high-security provider but hurts the low-security provider. Proposition 4 shows that it is *not always* the case. The reason is that information security rating generates two effects on the competition: (1) It eliminates the free riding problem. This effect helps two service providers to differentiate themselves.[1] Thus, the information security rating can benefit both service providers when both types of customers are not significantly differentiated ($\theta < \frac{5}{4}$). (2) It can intensify the competition in Period 1. In Case NR, when $\theta > 2$, the high-security provider can extract all the surplus from the high-type customer while the low-security provider can charge a high price by free-riding on the high-security provider. However, these benefits for both service providers are gone when the information security rating is provided. When it is hard to enhance the security (c is large), it will be useful for service providers to soften their competition. Thus, the information security rating, which can intensify the competition, may hurt both service providers. The following table gives numerical examples to illustrate the results of Proposition 4.

	θ	c	With risk rating	Without risk rating	Comparison
$\lambda = 0.2$, $V = 1$	1.2	1	$\pi_l^* = 1.64$, $\pi_h^* = 1.6416$	$\pi_l^* = 1.6395$, $\pi_h^* = 1.6379$	RR Benefits both vendors
	3	1	$\pi_l^* = 1.64$, $\pi_h^* = 1.8$	$\pi_l^* = 2.0869$, $\pi_h^* = 2.0969$	RR hurts both vendors
	3	0.2	$\pi_l^* = 1.8$, $\pi_h^* = 2.6$	$\pi_l^* = 2.4344$, $\pi_h^* = 2.4844$	RR Benefits the high-security vendor but hurts the low-security one
	1.5	1	$\pi_l^* = 1.64$, $\pi_h^* = 1.65$	$\pi_l^* = 1.6425$, $\pi_h^* = 1.64$	

Proposition 5. The information security rating does not affect the low-type customer, whose net surplus is always zero. It benefits the high-type customer except when $\theta > 12$, $\frac{8\theta}{3(3\theta-4)} < \lambda < 1$, and $V\lambda\theta < c \le \frac{V\lambda^2(\theta-12)}{8(1-\lambda)}$.

[1] In Case R, $e_h^* - e_l^* = \frac{V\lambda}{c}(\theta-1)$. In Case NR, $e_h^* - e_l^* = \frac{V\lambda}{2c}(\theta-1)$ for both S1 and S2. Clearly, $\frac{V\lambda}{c}(\theta-1) > \frac{V\lambda}{2c}(\theta-1)$, showing that the difference between e_h^* and e_l^* in Case R is larger than that in Case NR.

This result is different from Shapiro (1986), which showed that improved information *always* helps the high-type customer. The reason is that Shapiro (1986) assumed that the market is fully competitive with no profit for the sellers while we do not make such an assumption. Footnote 10 of Shapiro (1986) suggested that modeling heterogeneous sellers would permit the analysis of issues not modeled in that paper. The sellers in our paper are heterogeneous.

Intuitively, information security rating helps the high-type customer to choose the high-security service provider, and thus benefits the high-type customer. Hence, it seems quite counterintuitive that the information security rating can hurt the high-type customer. The reasons are as follows. Although information security rating encourages the high-security service provider to enhance its security, it can reduce the low-security service provider's effort on its security (when $\theta > 4$, see Proposition 3).Then, the high-type customer's alternative choice (low-security service provider) in Period 2 is worse than that when the rating is not provided. This means that the high-security provider need not give the high-type customer a high net surplus to lobby it not to choose the low-security provider. Therefore, the information security rating can hurt the high-type customer.

Proposition 4 and Proposition 5 have important managerial implications for the business model of the information security rating industry. For examples, the Moody's rating service charged service providers to conduct the assessment and also charged customers interested in the providers rating (the ratings were not publically available, but rather were provided for a fee). Our results suggest that it is not a good business model under certain conditions (for example, when both service providers are hurt by the information security rating). As shown above, the information security rating has quite subtle effects on competition, the business application service providers, and customers. The information security rating agencies must understand these effects to assess the customers and service providers willingness to pay for the rating service. Now, we examine the impacts of information risk rating on social welfare, which is the total surplus of vendors and consumers (that is, a sum of vendor profits and consumer surplus).

Proposition 6. Information security rating increases the social welfare.

Information security rating is a relatively new service compared to credit rating. In 1931, the credit rating was firstly endorsed by the Office of the Comptroller of the Currency, which required banks to use current market prices for all the bonds on their balance sheet rated below "investment grade". In 1936, the OCC went further and restricted banks from buying bonds below "investment grade". However, the information security rating is still not officially endorsed by the government. Proposition 6 suggests that social planners should encourage the information security rating through public policy initiatives.

6. CONCLUSION

There is growing interest in many industries for vendor information security rating services, which enabled enterprise customers to obtain risk assessments of their service providers. We investigate the impact of such risk rating services on customers, service providers and social welfare.

Intuitively, many may conclude that information security ratings should benefit the high-security service providers and hurt the low-security ones. But, we find that this is not always the case - information security ratings can hurt both high-security and low-security service providers. This occurs when the absence of a security rating softens the competition allowing the low-security service provider to appear identical to the high-security service provider. In that case, the low-security provider is able to charge a higher price than otherwise and the high-security service provider is able to avoid providing a positive net surplus to the high-type customer to guarantee that the customer does not choose the low-security provider. Therefore, it is possible that the information security rating can intensify competition and hurt both service providers. On the other hand, in some cases information security ratings can benefit both service providers. For example, in cases where the high-type customer is not significantly different from the low-type customer, it is useful for both service providers to differentiate their services though security to avoid head-to-head price competition. Since ratings clearly reveal the service quality of providers to customers, it helps service providers to differentiate themselves and thus can benefit both of them.

Prior literature showed that improved information always benefits the high-type customer (Shapiro 1986). Our model shows that information security rating can hurt the high-type customer. This is because our model captures competition between heterogeneous providers while Shapiro (1986) assumed homogeneous providers where profit is competed away. Hence, the improved information did not affect the competition in Shapiro's model. We consider a duopolist competition, where both service providers can earn a positive profit. We find that the information security ratings have subtle effects on the competition. When the rating is provided, it may reduce the low-security service provider's incentives to invest in security.

This reduces the quality of the alternative choice of the high-type customer. Thus, the high-security service provider will not give a sufficiently large net surplus to lure the high-type customer. This explains why the high-type customer can be hurt by an information security rating of providers.

Although the information security rating has subtle effects on service providers and customers respectively, it always increases the social welfare. The policy implication is that the information security rating should be encouraged by social planners.

Risk rating is a marketing tool. Future research can compare different marketing tools, e.g. a comparison between risk rating and advertisement.

REFERENCES

[1] Arora, A., R. Telang, and H. Xu. 2008. "Optimal Policy for Software Vulnerability Disclosure", *Management Science*, 54(4), 642-656.
[2] Arora, A., J. P. Caulkins, and R. Telang. "Sell First, Fix Later: Impact of Patching on Software Quality", *Management Science*, 52(3), 465-471.
[3] August, T., and T. I. Tunca. 2006. "Network Software Security and User Incentives", *Management Science*, 52(11), 1703-1720.
[4] August, T., and T. I. Tunca. 2008. "Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions", *Information Systems Research*, 19(1), 48-70.
[5] Bhargava, H., and V. Choudhary. 2001. "Information Goods and Vertical Differentiation", *Journal of Management Information Systems*, 18(2), 89-106.
[6] Bhargava, H., and V. Choudhary. 2008. "Research Note: When is Versioning Optimal for Information Goods?" *Management Science*, (forthcoming).
[7] Calder, A., J. V. Bon, and V. Haren. 2006. "Information Security Based on ISO 27001/ISO 17799: A Management Guide", Van Haren Publishing, Zaltbommel, Netherlands.
[8] DiRomualdo, A., and V. Gurbaxani. 1998. "Strategic Intent for IT Outsourcing", *Sloan Management Review*, 39(4), 67-80.
[9] Gal-Or, E. and Ghose, A. (2005) "The Economic Incentives for Sharing Security Information", *Information Systems Research*, (16)2, pp. 186-208.
[10] Kannan, K., and R. Telang. 2005. "Market for Software Vulnerabilities? Think Again", *Management Science*, 51(5), 726-740.
[11] Kark, K. 2008. "Can Moody's Solve Your Third Party Assessment Problem?" http://blogs.forrester.com/srm/2008/05/can-moodys-solv.html.
[12] Kliger, D., and O. Sarig. 2000. "The Information Value of Bond Ratings", *The Journal of Finance*, 55(6), 2879-2902.
[13] Macura, I. and E. Johnson. 2009. "Information Risk and the Evolution of the Security Rating Industry," Working Paper, Tuck School of Business at Dartmouth College. http://mba.tuck.dartmouth.edu/digital/Research/ResearchProjects/InfoRR7.pdf
[14] Muth, J. F. 1961. "Rational Expectations and the Theory of Price Movements", *Econometrica*, 29(3), 315-335.
[15] Shapiro, C. 1986. "Investment, Moral Hazard, and Occupational Licensing", *The Review of Economic Studies*, 53(5), 843-862.
[16] Stoneburner, G., A. Goguen, and A. Feringa. 2002. "Risk Management Guide for Information Technology Systems", National Institute Standards and Technology (NIST) Special Publication 800-30.

1. Proof of Proposition 1

Proof. $d(\pi_l)/de_l = d\left(2p_l - ce_l^2\right)/de_l = d\left[2V(1-\lambda+\lambda e_l) - ce_l^2\right]/de_l = 2V\lambda - 2ce_l$. Hence, $d(\pi_l)/de_l = 0$ leads to $e_l^* = V\lambda/c$. $d\pi_h/de_h = d\left(2p_h - ce_h^2\right)/de_h = d\left[2V\theta\lambda(e_h - e_l) + 2V(1-\lambda+\lambda e_l) - ce_h^2\right]/de_h = 2V\theta\lambda - 2ce_h$.

Hence, $d\pi_h/de_h = 0$ leads to $e_h^* = V\theta\lambda/c$. Inserting e_l^* and e_h^* in (1) and (2) gives p_l^*, p_h^*, π_l^*, and π_h^*.

3. Proof of Proposition 2

Proof. In the first scenario (S1), $p_i = V\theta(1-\lambda) + \frac{1}{2}\lambda\theta V\left[E(e_l) + E(e_h)\right]$, $p_l = V(1-\lambda+\lambda e_l)$, thus $\pi_l = \frac{1}{2}p_i + p_l - ce_l^2 = \frac{1}{2}\left[V\theta(1-\lambda) + \frac{1}{2}\lambda\theta V\left[E(e_l) + E(e_h)\right]\right] + V(1-\lambda+\lambda e_l) - ce_l^2$. Since customers form correct expectations

on e_l and e_h, we have $E(e_l)=e_l$ in equilibrium. Inserting $E(e_l)=e_l$ in π_l and solving the F.O.C. for e_l^*, we may get $e_l^*=V\lambda(4+\theta)/(8c)$. Using a similar analysis, we may get $e_h^*=5V\theta\lambda/(8c)$. Inserting e_l^* and e_h^* in p_i, p_h, p_l, π_l, and π_h, we may get p_i^*, p_h^*, p_l^*, π_l^*, and π_h^*. Using a similar argument, we may get results for the second scenario (S2).

The difference between π_h^* in S1 and S2 is $(\pi_h^*\mid \text{S1})-(\pi_h^*\mid \text{S2})=\frac{V}{64c}(\theta-2)\left[32c(1-\lambda)+V\lambda^2(22+3\theta)\right]$. Clearly, it is greater than 0 when $\theta>2$. Further, $(\pi_l^*\mid \text{S1})-(\pi_l^*\mid \text{S2})=\frac{V}{64c}(\theta-2)\left[32c(1-\lambda)+V\lambda^2(14+11\theta)\right]>0$ when $\theta>2$.

4. Proof of Proposition 3

Proof. We use the results of Proposition 1 and Proposition 2. $(e_h^*\mid \text{Case R})-(e_h^*\mid \text{S1, Case NR})=3V\theta\lambda/(8c)>0$, $(e_h^*\mid \text{Case R})-(e_h^*\mid \text{S2, Case NR})=V\lambda(2\theta-1)/(4c)>0$. $(e_l^*\mid \text{Case R})-(e_l^*\mid \text{S1, Case NR})=V\lambda(4-\theta)/(8c)\geq 0$ when $\theta\leq 4$ but <0 when $\theta>4$, $(e_l^*\mid \text{Case R})-(e_l^*\mid \text{S2, Case NR})=V\lambda/(4c)>0$.

5. Proof of Proposition 4

Proof. When $\theta>2$, the equilibrium is S1 in Case NR (see proof of Proposition 2). $(\pi_h^*\mid \text{Case R})-(\pi_h^*\mid \text{S1, Case NR})=\frac{V}{64c}\left[V\lambda^2(45\theta^2-112\theta+96)-32c(\theta-2)(1-\lambda)\right]$ is greater than zero when $c>\frac{V\lambda^2\left[96+(45\theta-112)\theta\right]}{32(\theta-2)(1-\lambda)}$, and less than or equal to zero otherwise.

$(\pi_l^*\mid \text{Case R})-(\pi_l^*\mid \text{S1, Case NR})=\frac{V}{64c}[-V\lambda^2(11\theta^2+8\theta-48)-32c(\theta-2)(1-\lambda)]<0$. When $1<\theta\leq 2$, the equilibrium is S2 in Case NR (see proof of Proposition 2).

$(\pi_h^*\mid \text{Case R})-(\pi_h^*\mid \text{S2, Case NR})=\frac{V^2\lambda^2}{16c}(12\theta^2-24\theta+13)>0$ in $\theta\in(1,2]$.

$(\pi_l^*\mid \text{Case R})-(\pi_l^*\mid \text{S2, Case NR})=\frac{V^2\lambda^2}{16c}(5-4\theta)>0$ in $\theta\in(1,\frac{5}{4})$ but ≤ 0 in $\theta\in[\frac{5}{4},2]$.

6. Proof of Proposition 5

Proof. Let ns_h^C be the net surplus of the high-type customer in Case C ($C=NR$, R).

$ns_h^R=2U(t_H,s_H,p_h)=\frac{2V}{c}(\theta-1)(c-c\lambda+V\lambda^2)$. When $1<\theta\leq 2$,

$ns_h^{NR}=U(t_H,p_i)+U(t_H,s_H,p_h)=\frac{V}{4c}(\theta-1)\left[8c(1-\lambda)+V\lambda^2(5+\theta)\right]$. $ns_h^R-ns_h^{NR}=\frac{V^2\lambda^2}{4c}(4\theta-\theta^2-3)>0$. When $\theta>2$,

$ns_h^{NR}=U(t_H,p_i)+U(t_H,s_H,p_h)=0+U(t_H,s_H,p_h)=\frac{V}{8c}(\theta-1)\times\left[8c(1-\lambda)+V\lambda^2(4+\theta)\right]$.

$ns_h^R-ns_h^{NR}=\frac{V}{8c}(\theta-1)\left[8c(1-\lambda)+V\lambda^2(12-\theta)\right]>0$ when $c>\frac{V\lambda^2(\theta-12)}{8(1-\lambda)}$. According to Assumption 1, $c>V\lambda\theta$. Only when $\frac{V\lambda^2(\theta-12)}{8(1-\lambda)}>V\lambda\theta$, $V\lambda\theta<c\leq\frac{V\lambda^2(\theta-12)}{8(1-\lambda)}$ is possible. Solving the inequality $\frac{V\lambda^2(\theta-12)}{8(1-\lambda)}>V\lambda\theta$, we get $\theta>12$ and $\frac{8\theta}{3(3\theta-4)}<\lambda<1$.

7. Proof of Proposition 6

Proof. Let SW^C be the social welfare in Case C (C=*NR, R*). Note that the net surplus of the low-type customer is zero, we have $SW^R=ns_h^R+\pi_h^*+\pi_l^*=\frac{V}{c}\left[2c(\theta+1)(1-\lambda)+V\lambda^2\left(1+\theta^2\right)\right]$..

When $\theta>2$, $SW^{NR}=ns_h^{NR}+\pi_h^*+\pi_l^*=\frac{V}{32c}\left[32c(2\theta+1)(1-\lambda)+V\lambda^2(8+8\theta+19\theta^2)\right]$;

$SW^R-SW^{NR}=V(1-\lambda)+\frac{V^2\lambda^2}{32c}(13\theta^2-8\theta+24)>0$. When $1<\theta\leq 2$, $SW^{NR}=\frac{V}{8c}\left[16c(\theta+1)(1-\lambda)+V\lambda^2(5+6\theta+4\theta^2)\right]$;

$SW^R-SW^{NR}=\frac{V^2\lambda^2}{8c}(4\theta^2-6\theta+3)>0$ in $\theta\in(1,2]$.